サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和2年
6月4日
Vol.46

テレワークのサイバーセキュリティ対策

第2報

新型コロナウイルス感染症対策として、テレワークの活用に関するセキュリティ対策のポイントを『サイバーセキュリティだよりVol.41』において紹介しているところですが、今回は「緊急事態宣言解除」を受けて、テレワークからオフィスワークへ戻る際の対策やチェックリストの活用等について紹介します。

～オフィスワークに戻る際の脅威～

一般家庭のネットワーク環境は、職場のネットワーク環境と比較すると、外部からの攻撃に対してセキュリティ対策のレベルが低いと考えられます。

テレワークで使用した端末等がウイルスに感染してしまっている場合、そのまま職場のネットワークに接続してしまうと…

感染拡大のおそれがあります!!

～　対　策　～

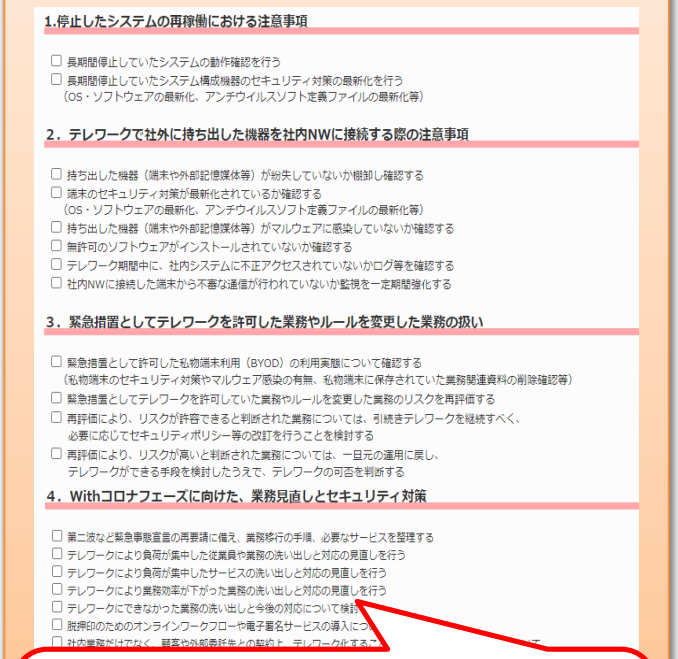
テレワークで利用した端末や外部記録媒体（USBメモリ等）を、職場のネットワーク等に接続する前に、セキュリティソフトでフルスキャンを行いましょう。

また、接続する端末等については、OSや各ソフトウェアのアップデートも行いましょう。

個人の端末から職場の端末にデータを移動する際は、職場に手続きを確認し、指定された方法で行いましょう。

テレワークとオフィスワークを考慮した情報セキュリティーポリシーや端末等の利用ルールの見直しも検討しましょう。

～セキュリティ・チェックリストの活用～



1.停止したシステムの再稼働における注意事項

□ 長期間停止していたシステムの動作確認を行う
□ 長期間停止していたシステム構成機器のセキュリティ対策の最新化を行う
（OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等）

2．テレワークで社外に持ち出した機器を社内NWに接続する際の注意事項

□ 持ち出した機器（端末や外部記憶媒体等）が紛失していないか棚卸し確認する
□ 端末のセキュリティ対策が最新化されているか確認する
（OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等）
□ 持ち出した機器（端末や外部記憶媒体等）がマルウェアに感染していないか確認する
□ 無許可のソフトウェアがインストールされていないか確認する
□ テレワーク期間中に、社内システムに不正アクセスされていないかログ等を確認する
□ 社内NWに接続した端末から不審な通信が行われていないか監視を一定期間強化する

3．緊急措置としてテレワークを許可した業務やルールを変更した業務の扱い

□ 緊急措置として許可した私物端末利用（BYOD）の利用実態について確認する
（私物端末のセキュリティ対策やマルウェア感染の有無、私物端末に保存されていた業務関連資料の削除確認等）
□ 緊急措置としてテレワークを許可していた業務やルールを変更した業務のリスクを再評価する
□ 再評価により、リスクが許容できると判断された業務については、引続きテレワークを継続すべく、必要に応じてセキュリティポリシー等の改訂を行うことを検討する
□ 再評価により、リスクが高いと判断された業務については、一旦元の運用に戻し、テレワークができる手段を検討したうえで、テレワークの可否を判断する

4．Withコロナフェーズに向けた、業務見直しとセキュリティ対策

□ 第二波など緊急事態宣言の再要請に備え、業務移行の手順、必要なサービスを整理する
□ テレワークにより負荷が集中した従業員や業務の洗い出しと対応の見直しを行う
□ テレワークにより負荷が集中したサービスの洗い出しと対応の見直しを行う
□ テレワークにより業務効率が下がった業務の洗い出しと対応の見直しを行う
□ テレワークにできなかった業務の洗い出しと今後の対応について検討
□ 脱押印のためのオンラインワークフローや電子署名サービスの導入につ
□ 社内業務だけでなく、顧客や外部委託先との契約上、テレワーク化する

特定非営利活動法人（NPO）日本ネットワークセキュリティ協会（JNSA）のホームページ（https://www.jnsa.org/telework_support/telework_security/index.html）に掲載されています。

相談窓口

参考：独立行政法人情報処理推進機構セキュリティセンター（IPA）
https://www.ipa.go.jp/security/announce/telework.html

愛媛県警察本部サイバー犯罪対策課　TEL089-934-0110㈹